The "Darth" Side of Technology Use:

An Inductively Derived Typology of Cyberdeviance

SRINIVASAN VENKATRAMAN
The Boeing Company
3860 Faber Place Dr, North Charleston 29405, U.S.
Email: srini@srinivenkatraman.com

CHRISTY M. K. CHEUNG
Department of Finance and Decision Sciences, School of Business,
Hong Kong Baptist University, Kowloon Tong, Hong Kong S.A.R.
Email: ccheung@hkbu.edu.hk

ZACH W. Y. LEE
Durham University Business School, Durham University,
Mill Hill Lane, Durham, DH1 3LB, United Kingdom
Email: zach.lee@durham.ac.uk

FRED D. DAVIS
Rawls College of Business, Texas Tech University
703 Flint Avenue, Lubbock, TX 79409, U.S.
Email: fred.davis@ttu.edu

VISWANATH VENKATESH
Sam M. Walton College of Business, University of Arkansas
228 Business Building Fayetteville, AR 72701, U.S.
Email: vvenkatesh@vvenkatesh.us

[Accepted in **Journal of Management Information Systems** at 09 August 2018]

SRINIVASAN VENKATRAMAN (srini@srinivenkatraman.com) is a Chief Data Scientist for The Boeing Company. He leads a team of data scientists in designing, developing, and deploying machine learning and artificial intelligence algorithms in engineering, manufacturing, and factory operations. Currently, Srinivasan is developing predictive analytics solutions for industrial robotics to predict machine downtime and machine defects, developing image/video analytics for identifying and predicting defects for quality inspection, developing predictive analytics solutions for supply chain processes, and developing deep learning/computer vision algorithms for engineering design and a variety of other manufacturing processes. Prior to joining Boeing, Srinivasan was an information systems faculty at Washington State University. Srinivasan has a Bachelor's degree in Physics, Master's degree in Information Systems and a Ph.D. in Information Systems.

CHRISTY M. K. CHEUNG (ccheung@hkbu.edu.hk; corresponding author) is an Associate Professor at Hong Kong Baptist University. She earned a Ph.D. in Information Systems from the

College of Business at City University of Hong Kong. Her research interests include Technology Use and Well-Being, IT Adoption and Use, Societal Implications of IT Use, and Social Media. She has published over one hundred refereed articles in international journals, and conference proceedings, including *Decision Support Systems*, *Information & Management*, *Journal of Information Technology*, *Journal of Management Information Systems*, *Journal of the Association for Information Science and Technology*, *MIS Quarterly* and among others. Dr. Cheung is currently President of the Association for Information Systems (AIS-Hong Kong Chapter). She also serves as Editor-in-Chief of *Internet Research*.

ZACH W. Y. LEE (zach.lee@durham.ac.uk) is an Assistant Professor in Marketing at Durham University Business School. He holds a Ph.D. degree from Hong Kong Baptist University. His research interests include online consumer behaviors, organizational and societal implications of IT use, social media, and e-commerce. He has published in international journals such as *Information & Management*, *Journal of the Association for Information Science and Technology*, *Electronic Commerce Research and Applications*, and *Journal of Marketing Analytics*. Zach serves as an Associate Editor in *Internet Research*.

FRED D. DAVIS (fred.davis@ttu.edu) is Professor and Stevenson Chair in Information Technology at Texas Tech University. Dr. Davis earned his Ph.D. from MIT's Sloan School of Management, and he served on the Business School faculties of University of Michigan, University of Minnesota, University of Maryland, and University of Arkansas. His research interests include user acceptance of information technology, technology supported decision making, system development practices, and NeuroIS. His research has been published in *MIS Quarterly*, *Information Systems Research*, *Management Science*, *Journal of Applied Psychology*, *Journal of Applied Social Psychology*, *Organizational Behavior and Human Decision Processes*, and other leading journals.

VISWANATH VENKATESH (vvenkatesh@vvenkatesh.us), who completed his PhD at the University of Minnesota, is a Distinguished Professor and Billingsley Chair at the University of Arkansas. He is widely regarded as one of the most influential scholars in business and economics, both in terms of premier journal publications and citations (e.g., Thomson Reuters' highlycited.com, Emerald Citations, SSRN). His work has appeared in leading journals in human-computer interaction, information systems, organizational behavior, psychology, marketing, medical informatics, and operations management. His works have been cited about 80,000 times (Google Scholar) and 22,000 times (Web of Science). He developed and maintains an IS research rankings web site that has received many accolades from the academic community including AIS' Technology Legacy Award. He has served in editorial roles at various journals. He is a Fellow of the Association of Information Systems (AIS) and the Information Systems Society, INFORMS.

ABSTRACT: Cyberdeviance, *intentional use of information technology (IT) in the workplace that is contrary to the explicit and implicit norms of the organization, and that threatens the well-being of the organization and/or its members*, is an important research stream that has gained attention in academia and industry. Prior studies have treated different forms of cyberdeviance as different phenomena, resulting in a lack of a collective underlying conceptualization of cyberdeviance. This work *inductively and empirically* derives a typology of cyberdeviance with 439 respondents across three phases. Our results suggest that cyberdeviance varies along 3 dimensions: cyberdeviant behaviors that are *minor* versus *serious*; cyberdeviant behaviors that target *individuals* versus *organizations*; and cyberdeviant behaviors that require *low* versus *high technical skill*. We thus provide a comprehensive framework that fosters a logical linkage of various research programs related to cyberdeviance to guide future research investigation. The typology will help managers to distinguish different cyberdeviant behaviors and implement suitable interventions depending on the behavior.

KEY WORDS AND PHRASES: Cyberdeviance, workplace deviance, typology, systematics approach, multidimensional scaling, IS security threats, IS use, cyberslacking, cyberloafing, cyberaggression, unauthorized access and use of IT, computer abuse, inductive approach.

Introduction

Although information technology (IT) innovations continue to enhance individuals' lives at work and home, they increase vulnerability to harmful deviant activities [1, 11, 22, 30, 75]. A diverse array of such behaviors has begun to draw the attention of practitioners because of the huge costs incurred by such harmful activities. For instance, the nonwork use of IT in the workplace costs U.S. businesses over $60 billion in lost productivity annually [53]. In addition to these direct costs, there are indirect costs stemming from lawsuits and diminished brand image, consumer loyalty, and trust. Many of these deviant behaviors often go unreported, making the actual costs even higher [38, 58].

Cyberdeviance is defined as the intentional use of IT in the workplace that is contrary to the explicit and implicit norms of the organization, and that threatens the well-being of the organization and/or its members. Despite a growing body of work on cyberdeviance, divergent conceptualizations of deviant use of IT remain a significant challenge for scholars to theoretically advance this important stream of research [11, 22]. Prior research has not focused on the nature of deviant IT use behaviors themselves. There is thus a lack of understanding of the underlying dimensions of cyberdeviance. In addition, prior research has almost solely focused on a particular deviant IT use behavior and is fragmented across the technical, psychological, and organizational behavior literature [89]. For instance, Posey et al. [59] suggested that prior studies examined information protective behaviors in isolation and there is a lack of understanding of the complex psychological processes surrounding the overall superset of behaviors. Similarly, in the context of cyberdeviance, previous works treated different forms of deviant IT use as different phenomena leading to a separate body of literature for each form of deviant behavior at work

[e.g., 22, 32, 54, 67]. To date, there is a lack of an integrative conceptualization of cyberdeviance that logically describes and differentiates an overall set of deviant IT use behaviors.

The growing connectivity, ubiquity, portability, and boundary spanning nature of IT exacerbate the potential costs and risks of cyberdeviance [91]. Only recently have organizations begun to monitor and regulate employees' IT use in the workplace, but the effectiveness and unintended consequences of such countermeasures are uncertain. One possible explanation is that many organizations do not have a complete understanding of cyberdeviant behaviors and the threats they pose [89]. As many cyberdeviant activities are not yet recognized, there are few laws and regulations governing them or interventions to prevent them. Likewise, research on cyberdeviance has seriously lagged practice [66]. In order to provide guidance for practitioners to develop effective mitigation and intervention strategies to curb cyberdeviance, there is a need to identify the characteristics of different forms of deviant IT use in the workplace.

The systematics approach [44] has been widely used in the natural sciences (e.g., biology, ecology, zoology) to discover the diversity among behaviors and their classifications. This approach has also been used among IS researchers [34, 46, 59, 68] with the focus on classifying the similarities – and dissimilarities – among objects of interest from which functional studies and subsequent theoretical advancements can emerge [80]. For instance, Posey et al. [59] used a systematics approach to develop a formal taxonomy and classification schema for protective information security behaviors. Such an approach enhances our understanding of the behaviors of interest by describing and differentiating an overall set of behaviors [43, 45]. It also provides researchers with insight into why findings from research that focus on one or only a subset of behaviors may not apply to others [24, 25]. Given the wide range of deviant IT use behaviors in the workplace, the area of cyberdeviance can benefit from a systematic investigation by

developing an empirically based typology of cyberdeviance. Specifically, the typology will help identify the nature of cyberdeviance and place cyberdeviance in the broader theoretical context of IT use in the workplace. The typology can assist in the identification of theoretical paradigms to study negative use of IT at work. Because little to no empirical research to date has examined how cyberdeviant behaviors are related to one another or what dimensions might underlie such deviant IT use, the present work breaks new ground for researchers related to IT use. We followed both Robinson and Bennett's [63] approach and a systematics approach [59] to *inductively and empirically derive* a typology of cyberdeviance in 3 phases. In the first phase, we elicit a range of cyberdeviant behaviors that are prevalent in the workplace. In the second phase, we use multidimensional scaling (MDS) to determine the dimensional structure underlying the range of cyberdeviant behaviors. In the third phase, we identify, interpret, and label the resulting types of cyberdeviance.

The rest of the paper is organized as follows: first, we present a background on why typologies are valuable followed by the conceptualization of cyberdeviance; then, we discuss the method followed by results; and, we conclude with a discussion of theoretical and managerial contributions.

Importance of Typologies

A key problem of cyberdeviance research is the lack of an integrative conceptualization of cyberdeviance that logically describes and differentiates various employees' deviant IT use behaviors. Accordingly, we embraced a systematics approach [59] to develop a typology of cyberdeviance. A typology provides a comprehensive map of a domain of a phenomenon and the ability to understand it with varying degrees of orientation and organization [40]. Typologies function as theory and are the most basic type of theory [17, 21, 47]. The construction of

typologies is a fundamental aspect of the process of inquiry by means of which the range and depth of knowledge with respect to social phenomena can be expanded [47]. To study an area that is underdeveloped and that has many unsolved problems, the disciplined construction and utilization of typologies are often useful first steps [47, 63]. As research on cyberdeviance is in its infancy, a typological classification is vital to comprehend its myriad aspects. Gregor [21] notes that there is a need for the development of typologies as a meaningful way to assess new constructs and relationships and uncover new patterns in existing relationships in IS research. Researchers in the fields of organizational behavior [e.g., 23, 63], strategic management [e.g., 19, 40], operations management [e.g., 27, 48], and information systems [e.g., 18, 20, 60] have developed typologies to understand specific individual or organizational phenomena. Such typologies have typically had significant influence on subsequent research in the respective domains.

In the organizational behavior literature, Robinson and Bennett [63] *inductively* and *empirically derived* a typology of workplace deviance behaviors using MDS. MDS allows researchers to produce a typology using the perceptions of a diverse set of individuals who are blind to the purpose of a given study. In other words, this approach is less prone to researchers' biases than typologies developed through other methods [63]. Their typology triggered the development of common theories of workplace deviance that examine antecedents and consequences of various deviance behaviors, resulting in a richer understanding of the underlying dynamics of workplace deviance behaviors [e.g., 2, 42, 56, 94]. Likewise, a systematic and *inductively* derived typology of cyberdeviance could be a starting point to understand the complex phenomenon of cyberdeviance.

Based on our understanding, there is no systematically and empirically derived typology of cyberdeviance in the literature. Few attempts have been made to classify highly related phenomena, such as work deviance [63] or computer abuse [91]. Willison and Warkentin [91], based on previous literature, proposed an IS security threat vector taxonomy. The main purpose of their work was to discuss potential research areas for empirical investigation. Robinson and Bennett [63] derived a typology of employee deviance with the primary focus on traditional deviant behaviors at workplace, such as theft, workplace violence, and loafing. They systematically and empirically derived a typology of workplace deviance that varies along 2 dimensions: minor versus serious and interpersonal versus organizational. We believe that their typology provides a useful starting point for us to develop a typology of cyberdeviance. Specifically, our investigation and development of a typology of cyberdeviant behaviors will provide greater depth while also identifying underlying dimensions. We expect to advance the literature by identifying one or more IT-related dimensions in the typology of cyberdeviance.

Developing a typology of cyberdeviance through a systematics approach is important for several reasons. First, it will provide a theoretical framework to study a wide range of cyberdeviant behaviors under the broad research stream of cyberdeviance. This will help understand various aspects of cyberdeviance and integrate other related research programs by illuminating the similarities and differences across various cyberdeviant behaviors. Second, it will help identify potential causal relationships and contingency factors associated with the relationships. Finally, it will help managers devise effective interventions to mitigate the occurrence of cyberdeviant behaviors by evaluating each cyberdeviant behavior independent of the others, so that those behaviors with the most frequent occurrence and those that pose the greatest threat to organizations and their members can be dealt with first.

Conceptualization of Cyberdeviance

Workplace deviance is defined as *"voluntary behavior that violates significant organizational norms and in so doing threatens the well-being of an organization, its members, or both"* [63]. Organizational behavior researchers have long investigated deviant behaviors in the workplace [e.g., 6, 7, 15, 63, 64]. We build on Robinson and Bennett's [63] *inductive* approach and conceptualize cyberdeviance as IT use behaviors that violate organizational norms, that are intentional, that are performed by the employees, and that are potentially harmful to the organization and/or co-workers.

Determining what are good, right, or moral behaviors is based on the normative perceptions that exist in an organization [5, 61]. Norms specify what behaviors are appropriate based on whether they conform to the expectations within a particular organization [31, 81], which are defined and communicated by the dominant organizational coalition—i.e., leaders and executives [10, 64]. Non-conforming behaviors can cause harm to the organization and/or the employees in the organization [63]. Hence, cyberdeviance, here, is conceptualized as deviations that violate implicit and explicit organizational norms. Implicit norms include supervisors or colleagues' attitude or behavior related to cyberdeviance as well as norms that generally come from the organization's culture, whereas explicit norms include organizational control and policies for cyberdeviance.

Although there could be unintentional and unconscious acts of negative IT use that are not under one's volitional control, our conceptualization of cyberdeviance specifically deals with *intentional and purposeful actions* performed by employees. The characteristics of actions are also important features of our conceptualization of cyberdeviance. Our conceptualization of cyberdeviance focuses on at the *intent to perform the behavior* rather than the *intent to cause*

harm. Hence, the focus is on IT use itself regardless of whether it results in harmful consequences for individuals and/or organizations. Although cyberdeviant behaviors can be performed by outsiders to the organization, our conceptualization focuses on *employees within the organization*. Similarly, although cyberdeviance can be targeted toward individuals and institutions outside the organization, our conceptualization of cyberdeviance is aimed at *objects within the organization*.

Prior Studies on Cyberdeviance

The scope of cyberdeviance in organizations is quite broad. The deviant use of IT ranges from relatively benign behaviors, such as Internet browsing, listening to music, and nonwork emailing, to more damaging or illegal behaviors, such as illegal downloading, IT sabotage, hacking and unauthorized entry into co-workers or supervisors' computers. Appendix A summarizes key studies from 1997 to 2018[1] published in leading IS journals—i.e., *Information Systems Research, Journal of the Association for Information Systems, Journal of Management Information Systems,* and *MIS Quarterly*—related to the deviant use of IT in the workplace. This summary provides an overview of the prior IS research on the topic. Specifically, these journals have published papers investigating the risks from intentional activities, such as software piracy [e.g., 50, 54], cyberloafing [e.g., 32], malicious insider attacks [e.g., 35], data or identity theft [e.g., 3], and unethical IT use [e.g., 11, 67]. However, prior IS works have not been logically integrated in an overarching framework [89]. Similarly, there is no systematically and empirically derived typology of cyberdeviance in the organizational behavior literature. Prior studies have almost solely focused on one particular type of cyberdeviance. For example, Lim [36] used the social exchange and organizational justice perspectives to explain employees'

[1] Articles published or available as forthcoming in 2018 at the time of submission of this version of the paper are included.

engagement in cyberloafing (or cyberslacking). Weatherbee and Kelloway [88] studied cyberaggression, with a focus on interpersonal aggression at work.

Method

The main purpose of this work is to develop a typology of cyberdeviance. We followed Robinson and Bennett's approach [63] to *inductively* develop a typology of cyberdeviance in 3 phases. This approach is inductive and grounded in nature. By casting the net wide (wider than may have been done in the previous research), we allow the dimensions that emerge to be grounded in actual experience. Figure 1 depicts the 3-phase typology development process. The natural starting point for a systematics approach is to derive the major behaviors that comprise the typology. Thus, the objective of phase 1 was to derive the range of cyberdeviant behaviors that are prevalent in the workplace. To accomplish this, focus group interviews were conducted to elicit different cyberdeviant behaviors. Then, a systematics approach guided us to understand how behaviors were related to each other. The objective of phase 2 was to position the behaviors elicited in phase 1 within an n-dimensional space using MDS. Specifically, a different group of participants rated how similar or different each elicited cyberdeviant behavior was from the others. MDS was then used to derive the spatial configuration of the cyberdeviant behaviors based on the similarity/dissimilarity ratings to produce the n-dimensional taxonomy. The objective of phase 3 was to create meaningful labels for the different dimensions identified in phase 2. Specifically, a different group of participants provided labels for the dimensions and rated how each cyberdeviant behavior fits with the label descriptors. MDS-based regression analysis was then performed to derive the final labels that describe each dimension. The use of different participants in each of the phases of the study minimized participant bias and carryover effects. The procedures and ensuing results for each phase of the study are discussed next.

Phase	Typology Development Process	Sample	Process Outcome
Phase 1	Focus group interviews to elicit cyberdeviant behavior incidents	134 employees of a Fortune 100 company and 15 doctoral students and faculty members in a U.S. business school	54 cyberdeviant behavior incidents
Phase 2	Multidimensional scaling of cyberdeviant behavior incidents	240 employees from 5 U.S. organizations	A three-dimensional typology
Phase 3	Interpreting and labeling typology categories	4 doctoral students and 46 MBA students	3 bi-polar descriptors

Figure 1. The 3-phase Typology Development Process

Phase 1: Focus Group Interviews to Elicit Cyberdeviant Behavior Incidents

Participants

We sent an invitation to 525 employees of a Fortune 100 company to participate in this phase of the research. The supervisor forwarded our email invitation to his/her subordinates. The email stated that we sought volunteers to participate in an interactive group discussion forum about different ways they use IT. Of these 525 employees, 134 employees agreed to participate, thus resulting in a response rate of 26%. Of the 134 participants, 59% of the participants were men and the average age was 39. All participants were working full-time, the average tenure with the company was 7 years, and 106 participants had at least an undergraduate degree. Various job functions and business units were represented, thus helping us to obtain diverse viewpoints.

Procedure

Focus group sessions were conducted over a 3-day period on-site at 2 different locations of the company in a large metropolitan area in the U.S. We followed the guidelines and suggestions provided by Morgan [51] to conduct the focus group sessions. Participants were divided into 9

groups and each session was restricted to no more than 20 people, the number of participants in each group ranged between 12 and 18. Three focus group sessions were conducted each day between 11:00 a.m. and 2:00 p.m., and each session lasted between 40 minutes and 1 hour. At the beginning of each focus group session, the specific activities of the session were explained to the participants. Participants did not have prior knowledge about the research or the activities of the session. The moderator (one of the authors) followed a script to moderate the basic dialog of all sessions. The script was created to include no value judgments and aimed to be unbiased. A co-moderator, who was not involved in the research, kept track of time, facilitated the discussions, and took notes as needed. The facilitation of the discussion by the co-moderator who did not know the research or its objectives allowed the discussion to be free-flowing and yet not be steered in any particular direction that could be construed as biased. Participants were first given a sheet of paper and were asked to list at least 2 incidents of someone using IT inappropriately at work in the organization and briefly describe why they thought it was inappropriate. Each participant was then asked to describe the incidents followed by an open discussion of the complete list of incidents and why they were inappropriate behaviors. Participants were asked to share their views and not required to reach agreement. Every participant listed at least 2 incidents and the number of incidents listed by participants ranged from 2 to 12 across the 9 sessions. At the end of each session, a summary of the discussion was provided to the participants and they were asked to confirm that the summary was an accurate representation of the discussion. They were then given an opportunity to add any other ideas or provide comments prior to the end of the session. Based on the focus group sessions, a total of 132 statements describing cyberdeviant behaviors were compiled for further evaluation. As we asked our participants to state the cyberdeviant behaviors that others have performed in this

phase, we believe that this approach encourages participants to honestly voice their opinions and eliminate the fear of being stigmatized or being subject to social desirability bias.

Next, a group of 15 judges comprising doctoral students and faculty members in a U.S. business school, who did not have any prior knowledge about the current study, were asked to independently evaluate the 132 cyberdeviant statements. Specifically, the judges were asked to check for redundancy and verbosity, to paraphrase or remove statements as needed, and to make sure the statements were inclusive enough to be generalized across different populations and organizations. The judges were also given the definition of cyberdeviance and asked to rate each of the behaviors on the extent to which they fit the definition of cyberdeviance. Specifically, the judges separately rated whether these behaviors were voluntary, violated general organizational norms, and were potentially harmful to organizations and/or employees. Here are some examples of discarded items: *collecting other employees' discarded printouts from the trash; contributing content to hate websites; indulging in activities that violate consumer privacy; printing big files (hundreds of pages) from work printers that are not work related; scanning personal pictures using a scanner at work; stealing other employees' printouts.* The authors checked the consistency of the results from the 15 judges and finalized a list of 54 cyberdeviant behaviors (see Table 1).

Table 1. List of Cyberdeviant Behaviors

No.	Statement
1	Sending/receiving personal emails through work email system
2	Sending spam, chain, and mass emails through work email system
3	Sending/receiving personal instant messages through work instant messaging system
4	Harassing co-workers through emails and instant messages
5	Using unauthorized applications
6	Harming other computers and systems by sending big attachments, videos, music, etc.
7	Accessing pornography content
8	Downloading personal content into work computers
9	Downloading malicious content into work computers
10	Browsing away work time

11 Browsing unsanctioned websites
12 Browsing websites for personal purposes
13 Causing harm to work computer resources
14 Accessing illegal content
15 Gambling online
16 Listening to music, video, and webcast
17 Storing and retrieving personal files on work computers
18 Playing computer games
19 Playing online games
20 Accessing violent and hatred content
21 Stealing hardware and software resources
22 Access and intrusion to work computers and servers that are not authorized
23 Illegal copying and distributing licensed electronic materials
24 Listening to music (CDs, files on computers)
25 Damaging and destroying computer resources
26 Hacking and enabling outsiders to hack work computers
27 Smearing the company online through emails/discussion boards
28 Whistle blowing about the company electronically
29 Spreading rumors and gossips about co-workers electronically
30 Job search using company computer resources
31 Concealing identity online and deceiving co-workers
32 Deleting/modifying electronic company files, codes, data, etc.
33 Deceiving customers by falsifying information
34 Engaging in identity theft
35 Provide/distribute access to individuals not authorized to access
36 Selling company technology resources and making profit
37 Unauthorized access to co-workers' computers
38 Using company resources to engage in march madness, fantasy football, etc.
39 Making unauthorized Internet phone calls
40 Posting company information, files, code online for public access
41 Monitoring co-workers' use of computer resources
42 Harassing co-workers online in public
43 Engaging in personal business using work computer resources
44 Taking the data hostage or encrypting the data without permission
45 Destroying and damaging computer resources
46 Downloading files, code off the Internet and using it at work
47 Sniffing the network resources to find holes in networks
48 Using external non-work-related ISPs/proxy servers to connect to the Internet from work
49 Electronic copyright violations
50 Electronic intellectual property violations
51 Playing loud music on the computer
52 Providing computers and software to employees with harmful content
53 Competing with the company in buying/selling/accessing technology resources
54 Unauthorized installation and use software/hardware components

Phase 2: MDS of Cyberdeviant Behavior Incidents

Participants

Two hundred and forty employees across 5 different organizations[2] in the southeastern U.S. participated in phase 2. Emails were sent to 750 employees across all 5 organizations, each from 1 of 5 different industries, i.e., retailing, telecommunication, logistics, marketing, and transportation, using a list maintained by a research center at a U.S. university. A total of 240 participants, with an average age of 36 and working full-time, volunteered and participated in this study. Of the participants, 107 were women. All participants completed all the tasks, thus resulting in a response rate of 32%.

Procedure

The first step in deriving the typology using MDS was to create the psychological distances between behaviors. This was accomplished by specifying how similar or different each behavior was from the other behaviors. Each respondent was asked to rate a different set of 100 randomly generated pairs of statements from the 54 statements generated in the previous phase. Specifically, participants rated the degree of similarity or difference among each pair of statements using a 9-point Likert-type scale (1=very similar, 9=very different) in an online environment. For example, a participant might rate the degree of similarity/difference between "engaging in identity theft" and "sending personal emails". As there are n(n-1)/2 total pairs across all 54 statements (where n=54), the resulting 1,431 possible comparisons was deemed to be too cognitively demanding and complex for the respondents to process. Respondents could be asked to rate all possible comparisons in an MDS study, but prior research has typically used a subset of all possible comparisons to reduce the complexity of the task [e.g., 55, 63]. Using a subset of statement pairs has been shown to reduce respondent burnout, errors, and attrition, but

[2] All 5 organizations had at least 1,000 employees and 3 of the 5 belonged to the Fortune 500.

not have any adverse effect on the findings [63, 76]. Hence, we asked participants to rate 100 pairs of statements. The participants were then asked to specify the criteria that they used for their ratings.

The next step was to interpret the number of underlying dimensions that provide an optimal fit for the data. This was accomplished by deriving the spatial configuration of the various cyberdeviant behaviors on the basis of the perceived difference from the other behaviors as rated by the respondents. The greater the differences (i.e., higher the ratings on the pairs) between the cyberdeviant behaviors, the greater was the distance between them in the spatial configuration. First, a matrix of dissimilarities (54x54) among the cyberdeviant behaviors was constructed based on the ratings provided by the respondents. Next, a metric MDS analysis was conducted to create dimensional configurations related to 1, 2, 3, and 4 dimensions [33]. The metric MDS is a method for constructing the geometric configuration of the different dimensions based on the Euclidian distances [see 13, 33] among the cyberdeviant behaviors in a spatial spectrum.

Results

The metric MDS analysis was performed using the ALSCAL program in SPSS. Two fit indexes—stress index and distance correlation—were used to analyze the underlying dimensions created by the metric MDS analysis. The fit indexes are objective functions that represent the extent to which the derived configuration fit with the data. Specifically, the indexes show whether a particular n-dimensional configuration fits the cyberdeviant behaviors better than other n-dimensional configurations. Stress index is the square root of the normalized residual sum of squares for the dimensional solution and may have values from 0 to 1 and determines which dimensional configuration explains the most variance [33]. Given the various cyberdeviant behaviors, the smallest possible value of the stress index without an appreciable decline in stress

from 1 n-dimensional configuration to an n+1-dimensional configuration is determined. A scree plot of the stress indexes for all the dimensional solutions was created to assess the decline in stress indexes across the n-dimensional space. A scree plot is particularly useful when dealing with comparisons larger than 30 [33]. The second fit index, the distance correlation (R^2), provides the correlation between the transformed data and the distances provided by MDS, i.e., the higher the value of R^2, the better the fit.

Based on the dimension heuristic suggested by Kruskal and Wish [33], the stress indexes for 1, 2, 3, and 4 dimensions were assessed. The 1-dimensional configuration had a stress index of .43 and R^2 of .49; the 2-dimensional configuration had a stress index of .39 and R^2 of .56; the 3-dimensional configuration had a stress index of .26 and R^2 of .70; and the 4-dimensional configuration had a stress index of .22 and R^2 of .71. The stress index had a moderate drop from the 1-dimensional to the 2-dimensional configuration, a noticeable drop from the 2-dimensional to the 3-dimensional configuration, and leveled off from the 3-dimensional to the 4-dimensional configuration. The R^2 for the configurations also leveled off from the 3-dimensional to the 4-dimensional configuration. The scree plot also suggested that the stress indexes leveled off after the 3-dimensional configuration. The results indicated that the 3-dimensional typology provided the most parsimonious and definitive solution.

Phase 3: Interpreting and Labeling Typology Categories

Participants

Participants in this phase comprised 4 doctoral students and 46 full-time MBA students, with an average of 5 years of prior work experience. The average age was 32. The participants were informed about the activities a week prior to the session.

Procedure

As mentioned in the phase 2 discussion earlier, the respondents in phase 2, when rating the similarities or differences among the behaviors, also indicated the criteria (why they think the behaviors are similar or different) they used to provide the similarity/difference ratings. First, the 4 doctoral students, blind to the study, acted as judges and were asked to evaluate the criteria, and paraphrase and simplify them. For example, one of the respondents (from phase 2) specified that "I looked at them to see if they were similar in the degree of harm, risk potential in terms of how they can hurt different stakeholders in the company" and one of the judges had paraphrased the statement as *harming different stakeholders* and another judge had paraphrased the statement as *seriously hurting the co-workers*. The judges were then asked to provide potential labels or attributes that best describe the criteria by creating bi-polar indicators. The judges created 7 bi-polar descriptors based on the top 7 criteria: serious - not serious, harmful to individuals - not harmful to individuals, harmful to organization - not harmful to organization, moral - immoral, visible to others - not visible to others, low technical skill required - high technical skill required, useful to the individual - not useful to the individual. Then, the 46 MBA students rated each of the 54 cyberdeviant behaviors on each of the bi-polar descriptors using a 9-point Likert-type scale. For example, one of the bi-polar descriptors ranged from "this behavior is not harmful to organizations" (1) to "this behavior is harmful to organizations" (9).

Results

The first step toward the interpretation of the dimensions was to specify the average of the MBA respondents' ratings of the 54 behaviors on each of the 7 bi-polar descriptors. Regression analysis was then performed to determine the relationship between the mean ratings of each cyberdeviant behavior along each bi-polar descriptor—i.e., the ratings of the MBA students—

and the 3-dimensional configuration—i.e., stimulus coordinates for every behavior on the 3 dimensions. The mean ratings were the dependent variables and the coordinates of the configuration were the independent variables in the regression model. The coordinates[3] were the actual position—i.e., distance from the origin—of the cyberdeviant behaviors in the 3-dimensional configuration. The regression specifically tests to see if the bi-polar indicators have a relationship to the position of the cyberdeviant behaviors in the 3-dimensional space such that the bi-polar indicators can be linked to the 3 dimensions. The final bi-polar labels will be chosen based on the squared multiple correlations and the beta weights from the regression analysis. A bi-polar descriptor having a high squared multiple correlation in relation to the stimulus coordinates and a high beta weight on a specific dimension can be considered as a descriptor for that dimension. The regression line corresponding to each of the bi-polar descriptors is in the form:

$$a + b_1x_1 + b_2x_2 + b_3x_3$$

where b_1, b_2, and b_3 are the beta coefficients or cosine values of the angle between the regression line and each of the dimensional axes; and x_1, x_2, and x_3 are the coordinates of the cyberdeviant behavior in the three-dimensional space.

In interpreting the dimensions and their respective bi-polar indicators, the multiple correlations must be high—i.e., variance explaining the bi-polar descriptor by the coordinates—and the regression weights should be high—i.e., the angle between the dimensional axis and the regression line representing the bi-polar indicator is small [33]. Table 2 shows the results.

[3] Each behavior on the 3-dimensional space will have 3 coordinates corresponding to their position in the space. For example, say the 3 coordinates are x, y and z. Then, each of the 54 statements will correspond to a point in the 3-dimensional space (x_i, y_i, z_i), where i ranges from 1 to 54.

Table 2. Results of Regression for the Dimensions for Bi-polar Descriptors

Bi-polar descriptors	Regression weights			Squared Multiple Correlation
	Dimension 1	Dimension 2	Dimension 3	
Minor-serious	0.77	0.34	-0.16	0.76
Harmful to organization-not harmful to organization	0.42	0.67	0.39	0.64
Harmful to individuals-not harmful to individuals	-0.46	-0.71	0.21	0.72
Moral-Immoral	0.32	-0.41	0.07	0.51
Visible to others-not visible to others	-0.23	-0.03	-0.11	0.30
Low technical skill-high technical skill required	0.38	0.36	-0.80	0.84
Useful to the individual-not useful to the individual	-0.12	-0.02	-0.09	0.22

Dimension 1. The largest regression weight on the first dimension was .77 (a regression weight of .77 corresponds to an angle of 40 degrees as cosine (40°) = .77) associated with the *minor - serious* bi-polar indicator and the corresponding squared multiple correlation was .76. This dimension was hence related to the *minor - serious* bi-polar indicator. Specifically, it suggested that one of the underlying dimensions for classifying cyberdeviant behaviors is whether the particular cyberdeviant behavior was minor or serious. Consequently, we labeled the first dimension "minor versus serious cyberdeviance."

Dimension 2. The most significant regression weight on the second dimension was -.71 on the *harmful to individual - not harmful to individual* bi-polar indicator and the corresponding value of squared multiple correlation was .72. The bi-polar indicator *harmful to organization - not harmful to organization* also had a high coefficient for this dimension (.67) with a multiple correlation coefficient of .64. As the bi-polar indicators *harmful - not harmful to individual* and *harmful - not harmful to organization* had relationships with dimension 2 in opposite directions (one was positive and the other was negative) and given both had high beta weight and multiple correlation on the same dimension, dimension 2 was a combined bi-polar indicator of harmful to organizations or individuals. Specifically, it suggested that one of the underlying dimensions for classifying cyberdeviant behaviors was whether the particular cyberdeviant behavior was

harmful to individuals or the organization. Collectively, we labeled this dimension "individual versus organizational cyberdeviance."

Dimension 3. The most significant regression weight on the third dimension was -.80 on the *low technical skill - high technical skill required* bi-polar indicator and the corresponding squared multiple correlation was .84. This suggested that one of the underlying dimensions for classifying cyberdeviant behaviors was whether or not one needed strong technical skill to engage in cyberdeviance. We, therefore, labeled the third dimension "low technical skill versus high technical skill cyberdeviance."

Figure 2 provides the 3-dimensional configuration of the taxonomy of cyberdeviance. Each axis in the configuration represents the 3 dimensions along with their respective bi-polar indicators. Observation of the 3-dimensional configuration supports the use of the above labels. Table 3 shows typical behaviors in each dimension in the typology.

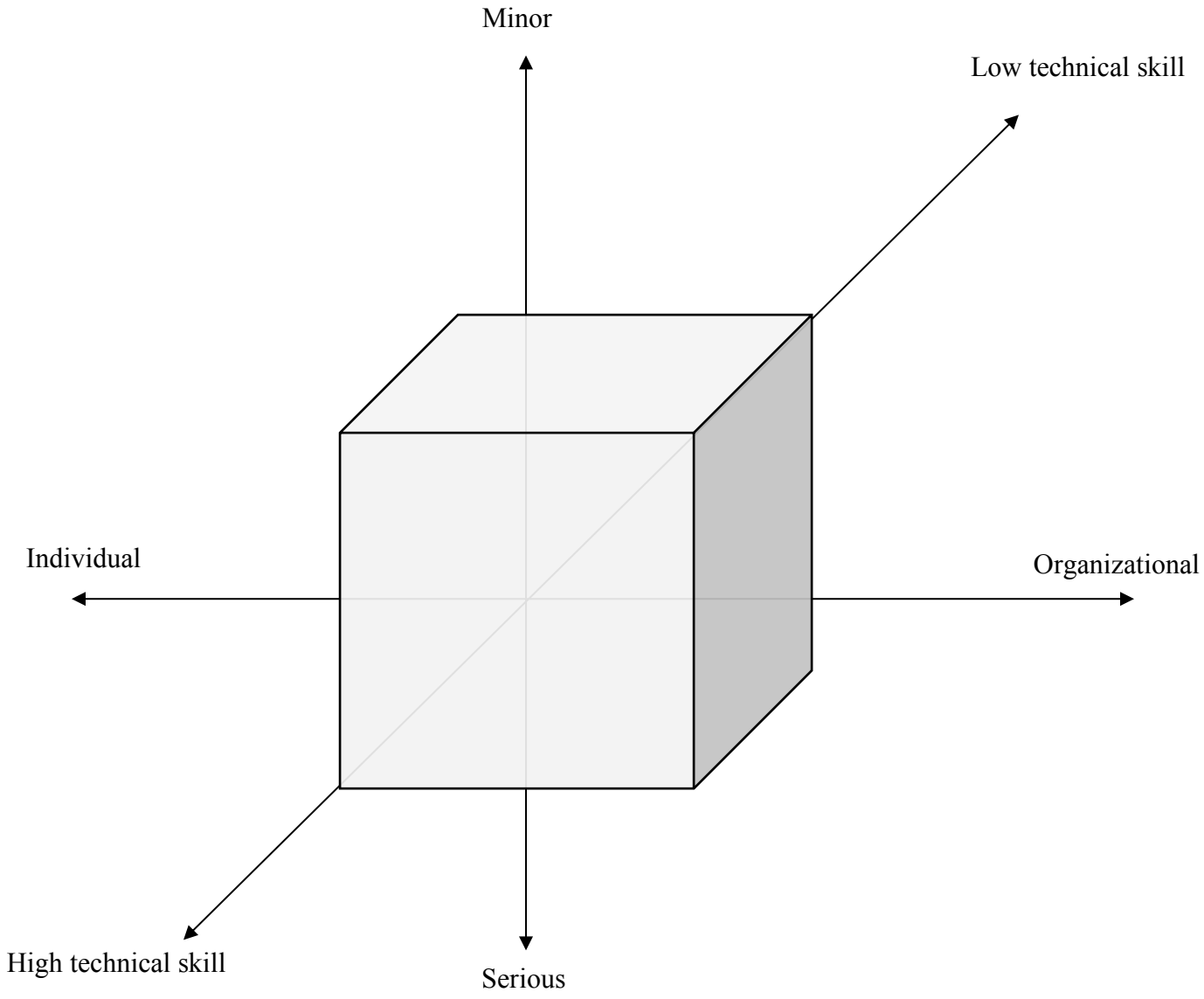

Figure 2. Three-Dimensional Typology of Cyberdeviance

Table 3. Typical Behaviors in Each Dimensional Configuration in the Typology*

	Individual	Organizational
Minor	**Low technical skill**	**Low technical skill**
	• Spreading rumors and gossips about co-workers electronically • Sending spam and mass email messages • Playing music loud on computers	• Sending/receiving personal emails • Browsing away work time • Playing computer games
	High technical skill	**High technical skill**
	• Concealing identity online and deceiving co-workers • Monitoring co-workers' use of computer resources • Providing damaged computer resources to employees	• Using external ISPs/proxy servers to connect to the Internet from work • Engaging in computer rage • Unauthorized installation of hardware and software in company computers
	Individual	**Organizational**
Serious	**Low technical skill**	**High technical skill**
	• Harassing co-workers through emails and instant messages • Distributing pornography content to co-workers • Distributing violent and hatred content online	• Posting critical company information online • Smearing the company online • Stealing company hardware and software resources
	High technical skill	**High technical skill**
	• Unauthorized access to co-workers' computers • Engaging in identity theft • Concealing identity and deceiving co-workers	• Spreading virus in work computers • Hacking and intrusion into computer resources • Encrypting company data and taking data hostage

*****These lists are not exhaustive. We provide some typical behaviors for each combination for illustrative purposes only.

Discussion

This work builds on an emerging stream of research on deviant use of IT in the workplace and develops a typology of cyberdeviance in a 3-phase research study. Following Robinson and Bennett [63] and a systematics approach [59], we *inductively* developed a typology of cyberdeviance with 3 dimensions, namely "*minor versus serious*", "*individual versus organizational*" and "*low technical versus high technical skill*", suggesting that cyberdeviant behaviors can be categorized based on whether they are minor or serious in nature, whether they affect the individuals or organizations, and whether low or high technical skill is required to engage in cyberdeviance. The results share some similarities with the typology of workplace deviance, but is unique in terms of the IT-specific dimension (i.e., low technical versus high

technical skill required). Based on the different combinations of the 3 dimensions, there are 8 categories of cyberdeviant behaviors. The categories can be connected to 4 existing streams of research in prior literature, namely *cyberslacking, computer abuse, unauthorized access and use of IT,* and *cyberaggression*.

Cyberslacking (or cyberloafing) refers to nonwork personal use of IT [90]. The categories of "*A minor form of organizationally oriented deviant use of IT with low technical skill*" and *"A serious form of organizationally oriented deviant use of IT with low technical skill*" are connected to cyberslacking. Some researchers considered cyberslacking as a form of "production deviance" [36] that can be accomplished relatively easily. This form of counterproductive workplace behavior [28, 52] can distract employees, thus affecting their productivity. All deviant IT use behaviors (e.g., *"sending/receiving personal emails and instant messages", "browsing websites for personal purposes", "listening to the music on the computer", "playing computer games"*) identified in the category of *"A minor form of organizationally oriented deviant use of IT with low technical skill"* are nonwork personal use of IT that affect productivity. Further, the results show that this form of cyberdeviance requires low technical skill, supporting the assumption of cyberslacking that is easy to perform. Some researchers, however, considered cyberslacking as a form of "property deviance" [9] that suggests that deviant IT use behaviors have the potential for consuming organizational resources (e.g., network or software). The deviant IT use behaviors (e.g., *"accessing pornography content", "accessing violent and hatred content", "playing online games"*) identified in the category of *"A serious form of organizationally oriented deviant use of IT with low technical skill"* are nonwork personal use of IT that can be easily performed but seriously drain organizational computing networks and bandwidth [87].

To conclude, cyberslacking is generally regarded as organizationally oriented deviant IT use with low technical skill required. The "production deviance" type of cyberslacking usually has minor impacts to the organization, whereas the "property deviance" type of cyberslacking has more serious impacts on the organization. These 2 types of cyberslacking behaviors have been well-studied in the organizational behavior literature [e.g., 36, 52, 95] but not in the mainstream IS literature (except [32]).

Computer abuse is a distinct stream of IS research that primarily focused on issues related to computer security, privacy, and fraud [39, 49, 70, 71, 91]. According to our review of papers published in leading IS journals (see Appendix A), most prior IS studies focused on this form of cyberdeviance [e.g., 3, 11, 35], probably because of its serious impact on organizations. All deviant IT use behaviors (e.g., *"hacking and intrusions into computer resources", "accessing illegal content", "stealing customer information and deceiving customers", "spreading virus in work computers"*) identified in the category of *"A serious form of organizationally oriented deviant use of IT with high technical skill"* is connected with the computer abuse literature. This stream of research has paid attention to serious IT-related criminal behaviors [e.g., 16] that target organizations. Further, most studies in this area have investigated control mechanisms intended to deter computer crimes [e.g., 4, 26, 49, 71, 72, 91]. This literature argues that computer crimes committed by employees can be prevented by sanctions and countermeasures [72], such as monitoring technology use [70], providing security awareness education and training [4], and strictly enforcing IT use policies and code of ethics [26]. Studies in this area are well-established and systematically organized in the IS literature [e.g., 37, 91].

Unauthorized access and use of IT refers to the violation of the right to access and use IT resources in organizations. All deviant IT use behaviors (e.g., *"making unauthorized Internet*

phone calls", "unauthorized installation of hardware and software in company computers", "using external ISPs/proxy servers to connect to the Internet from work") identified in the category of *"A minor form of organizationally oriented deviant use of IT with high technical skill"* is connected with the IS literature on unauthorized access and use. Similar to the computer abuse literature, existing works in IS mainly focused on interventions to reduce the violations of IT access and use in a nonintrusive manner [e.g., 82].

Cyberaggression represents a constellation of offensive behaviors and attitudes intending to intimidate, harass, or threaten a co-worker [57]. Cyberaggression has been extensively researched in prior research [e.g., 12, 14, 41, 69, 73]. However, most of these studies only focused on how cyberaggression negatively affected job performance and other task-related outcomes in the workplace [88]. Researchers seldom look at this form of cyberdeviance from the degree of impact (i.e., minor versus serious) and the technical skill required (i.e., low technical skill versus high technical skill). Compared with other forms of cyberdeviance, cyberaggression has been less systematically investigated in the IS literature.

Theoretical Implications

This work contributes to the IS literature in several ways. First, whereas a significantly large portion of the IS literature has been directed toward examining positive IT use, both in the workplace and society [65, 86], this work provided a parsimonious typology of cyberdeviance that can guide future research on negative use of IT at work. Recently, scholars in IS have argued for a rich conceptualization of system use by including the different patterns of IT use [62, 74, 86, 96]. Our typology will enable researchers to understand the relationships among the different types and subsequently, among the different behaviors. For example, all cyberdeviance behaviors that are potentially harmful to the organizations can be examined together to understand the

commonalities across them. This will in turn help develop a general theory of cyberdeviance by examining behaviors within and across the dimensions.

Second, we note that this work benefitted from using a systematics approach [59]. Specifically, we followed both Robinson and Bennett's [63] approach and a systematics approach [59] to *inductively* develop a typology of cyberdeviance in 3 phases. We identified that cyberdeviance varied along 3 dimensions and integrated numerous deviant IT use behaviors into a framework. The typology derived here makes a contribution to the literature by empirically validating the existing literature on workplace deviance and adding a new dimension that is IT-specific. In addition, our typology identified the underlying dimensions of cyberdeviance and thus clarified not only the different categories of deviant IT use behaviors, but also how these categories were related to one another. For example, our typology indicated that computer abuse behaviors, such as IT security and privacy violations, can be theoretically placed under the type of cyberdeviance that were serious, required high technical skill, and were harmful to organizations. Similarly, the typology illustrated that cyberslacking can be theoretically placed under the subset of behaviors that are minor and require low technical skill. To determine whether a cyberslacking behavior was a production-deviant or property-deviant activity, the degree of harm to organizations (minor versus serious) was an important indicator.

Third, this typology is useful in the development of general theories of cyberdeviance. Particularly, it created meaningful patterns out of the wide range of cyberdeviant behaviors by allowing us to describe and differentiate deviant IT use behaviors. It also facilitated integrating and positioning prior streams of research in the framework. Further, the typology allowed us to connect to the existing literature and understand the research status of various forms of cyberdeviance. For instance, the results clearly suggested that several deviant IT use behaviors

(e.g., cyberslacking, cyberaggression) have not been systematically investigated in the IS literature.

Limitations and Future Research

There are some limitations of this work that should be noted. The list of cyberdeviant behaviors generated was based on a single organization and the behaviors may differ in other organizations or organizations in other industries. However, employees from a wide range of job functions from software developers to administrative assistants and from various business units participated in the study that suggest that the results could potentially generalize across different populations. Further, as one of the authors was directly involved in the data collection, the biases of the researcher might have influenced the findings. However, the author followed a strict and unbiased script with no value statements, thus minimizing this concern; further, we believe that the use of multiple participants and multiple judges in each phase of the study minimized bias.

Another limitation was that respondents in phase 2 of the study evaluated only 100 pairs of behaviors. This made it difficult to render each individual's overall dimensional configuration, which requires all respondents to rate all possible pairs of behavior. As each individual's dimensional configuration might have been different, it could have been useful to understand the individual assessment of the different dimensions. However, as noted earlier, in addition to the prohibitive number of statement pairs as a constraint, prior research has consistently demonstrated that such use of subsets of pairs had no effect on the dimensional configuration.

Future research can build on our typology to investigate the motivations and consequences of the various categories of cyberdeviance. For instance, what are the motivations (or consequences) that are unique to specific cells in the typology? Existing theories or prior research could be most useful for this future research direction, which went as far as establishing

the typology, leaving an unanswered question: what are the motivational factors (or the diverse negative consequences) of these cyberdeviance behaviors and what is their generality and/or specificity relative to the typology categories?

Although we expect that the nature of the cyberdeviant behavior remains similar, the technologies involved may change over time because of the emergence of new technologies. For example, we identified that "sending/receiving personal emails" as one form of cyberslacking/cyberloafing behavior. The use of personal emails may become less often as people are changing the way they communicate with each other. Most people are now relying on instant messaging or social networking sites for instant communication rather than using emails. Future research should continue to explore how cyberdeviant behaviors change over time—these changes can be triggered in a variety of ways that include the evolution of platforms that may even create new paradigms of applications [see 93]. More broadly, given that technologies are used for productive purposes even outside the workplace [see 77] suggests the need to understand nonwork behaviors in a holistic way. As such investigations get underway, key contingencies, ranging from individual demographics to situational, cultural or psychological variables, will be important to incorporate [83, 84, 85, 92].

Managerial and Public Policy Implications

This work has important implications for managers. The typology developed here provided a comprehensive categorization of various cyberdeviant behaviors that were prevalent in the workplace. Our typology can potentially help managers to distinguish between various cyberdeviant behaviors and focus on the behaviors that have potentially serious outcomes first. The typology can help managers implement interventions based on the different subtypes of cyberdeviance. As each cyberdeviant behavior is largely different from other cyberdeviant

behaviors, different interventions can be designed to curb different behaviors. For example, monitoring can be implemented to curb serious behaviors, such as breaching the security or hacking, whereas some sort of incentive-based interventions can be implemented for more benign behaviors, such as cyberslacking.

Given the increase in cyberdeviance and the potential for more serious violations using IT, organizations are being asked to produce electronic artifacts, such as email and instant messages logs, in courts for legal proceedings and liabilities are becoming a cause for concern. In fact, damage from cyberdeviance and the potential liability for deviant IT use behaviors has become such a common occurrence that third-party insurance, popularly known as cyberinsurance, is flourishing [88, 97]. An implication for practice is that the typology can help disseminate the seriousness of the behaviors and potential for damage, which can be used in writing cyberinsurance policies. The typology can also help system designers to build better systems that prevent users from engaging in cyberdeviance. The dimensional attribute of low versus high technical skill supports the notion that different systems can be used for different cyberdeviant behaviors and hence, features of a specific system can be designed based on the type of cyberdeviant behaviors that users are more likely to engage in using that particular system.

The current work also has important implications for public policy. Judicial and legislative systems in the U.S. are now increasingly dealing with cases involving a wide range of IT-enabled deviant behaviors, including sexual harassment, theft, discrimination, financial frauds, spamming, hacking, illegal pornography, espionage, and sabotage [29, 78]. Laws for IT-based offenses have also been strengthened in the last decade or so. Many terms, such as cyberstalking, cyberextortion, and cyberharrasment, have been coined and are used as official judicial parlance for prosecution [79]. However, the technological advances and the sophistication in computer

crimes have limited the ability to carefully identify the victims, assess the damages, prosecute the perpetrators and most importantly, prevent the crimes. Legislation and enactment of statutes have typically occurred only after the computer crimes have been committed [79]. This typology can serve as a starting point and guide a discourse to prevent such crimes.

Cyberdeviance has also permeated into social, economic, educational, and political landscapes. Senators have resigned and political parties have been maligned getting caught up in cyberdeviant activities; innocent victims of IT-based sexual harassment have committed suicide; racially charged emails have been sent to minority students; and students have bullied other students via emails. This typology can guide public policy development by helping government and judicial systems in devising laws that govern the misuse of IT.

Conclusions

Despite the increased prevalence of cyberdeviance, researchers and practitioners have yet to gain a comprehensive understanding of this problem, which is vital in today's workplace. This work examined deviant IT use behaviors in the workplace and developed a typology of cyberdeviance in a 3-phase study. We used both Robinson and Bennett's [63] approach and a systematics approach [59] to inductively develop a typology that allowed us to connect the previously fragmented streams of research on various forms of cyberdeviant behaviors. As previously developed typologies across different fields of study have had a profound impact [e.g., 8, 18, 20, 60, 63] on advancing knowledge in the respective areas, we believe our typology can pave the way for a new line of inquiry in IS research regarding cyberdeviant behaviors and help in advancing our limited understanding of cyberdeviance. Our typology will also help managers to distinguish different types of cyberdeviant behaviors and focus organizational resources on curbing those that have potentially serious negative consequences. It will also help

managers to devise and implement interventions based on the attributes of the subtypes of cyberdeviance.

REFERENCES

1. Addas, S., and Pinsonneault, A. E-mail interruptions and individual performance: Is there a silver lining? *MIS Quarterly*, *42*, 2 (2018), 381-405.

2. Ashforth, B.E.; Schinoff, B.S.; and Brickson, S.L. "My company is friendly," "mine's a rebel": Anthropomorphism and shifting organizational identity from "what" to "who". *Academy of Management Review,* (forthcoming).

3. Banerjee, D.; Cronan, T.P.; and Jones, T.W. Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, *22*, 1 (1998), 31-60.

4. Barlow, J.; Warkentin, M.; Ormond, D.; and Dennis, A.R. Don't even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems,* (forthcoming).

5. Bennett, R.J.; Aquino, K.; Reed II, A.; and Thau, S. The normative nature of employee deviance and the impact of moral identity. In, Fox, S., and Spector, P.E., (eds.), *Counterproductive work behavior: Investigation of actors and targets*, Washington D.C.: APA Publishing, 2005, pp. 107-125.

6. Bennett, R.J., and Robinson, S.L. Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*, 3 (2000), 349-360.

7. Bennett, R.J., and Robinson, S.L. The past, present, and future of workplace deviance research. In, Greenburg, J., (eds.), *Organizational behavior: The state of the science*, Mahwah, NJ: Lawrence Erlbaum, 2003, pp. 247-282.

8. Bhattacherjee, A.; Davis, C.J.; Connolly, A.J.; and Hikmet, N. User response to mandatory IT use: A coping theory perspective. *European Journal of Information Systems,* (2018).

9. Blau, G.; Yang, Y.; and Ward-Cook, K. Testing a measure of cyberloafing. *Journal of Allied Health*, *35*, 1 (2006), 9-17.

10. Chatman, J.A. Matching people and organizations: Selection and socialization in public accounting firms. *Administrative Science Quarterly*, *36*, 3 (1991), 459-484.

11. Chatterjee, S.; Sarker, S.; and Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*, 4 (2015), 49-87.

12. Connolly, T.; Jessup, L.M.; and Valacich, J.S. Effects of anonymity and evaluative tone on idea generation in computer-mediated groups. *Management Science*, *36*, 6 (1990), 689-703.

13. Coxon, A.P.M., and Davies, P. *The user's guide to multidimensional scaling: With special reference to the MDS (X) library of computer programs*. London: Heinemann Educational Books, 1982.

14. D'Cruz, P.; Noronha, E.; and Lutgen-Sandvik, P. Power, subjectivity and context in workplace bullying, emotional abuse and harassment: Insights from postpositivism. *Qualitative Research in Organizations and Management: An International Journal*, *13*, 1 (2018), 2-9.

15. Dalal, R.S. A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology*, *90*, 6 (2005), 1241-1255.

16. Dhillon, G., and Moores, S. Computer crimes: Theorizing about the enemy within. *Computers & Security*, *20*, 8 (2001), 715-723.

17. Doty, D.H., and Glick, W.H. Typologies as a unique form of theory building: Toward improved understanding and modeling. *The Academy of Management Review*, *19*, 2 (1994), 230-251.

18. Earl, M. Knowledge management strategies: Toward a taxonomy. *Journal of Management Information Systems*, *18*, 1 (2001), 215-233.

19. Ellis, B., and Calantone, R. Understanding competitive advantage through a strategic retail typology. *Journal of Applied Business Research*, *10*, 2 (1994), 23-32.

20. Fiedler, K.D.; Grover, V.; and Teng, J.T.C. An empirically derived taxonomy of information technology structure and its relationship to organizational structure. *Journal of Management Information Systems*, *13*, 1 (1996), 9-34.

21. Gregor, S. The nature of theory in information systems. *MIS Quarterly*, *30*, 3 (2006), 611-642.

22. Guo, K.H.; Yuan, Y.; Archer, N.P.; and Connelly, C.E. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*, 2 (2011), 203-236.

23. Hagelskamp, C.; Hughes, D.; Yoshikawa, H.; and Chaudry, A. Negotiating motherhood and work: A typology of role identity associations among low-income, urban women. *Community, Work & Family*, *14*, 3 (2011), 335-366.

24. Hanisch, K.A., and Hulin, C.L. General attitudes and organizational withdrawal: An evaluation of a causal model. *Journal of Vocational Behavior*, *39*, 1 (1991), 110-128.

25. Hanisch, K.A.; Hulin, C.L.; and Roznowski, M. The importance of individuals' repertoires of behaviors: The scientific appropriateness of studying multiple behaviors and general attitudes. *Journal of Organizational Behavior*, *19*, 5 (1998), 463-480.

26. Harrington, S.J. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20*, 3 (1996), 257-278.

27. He, J., and Fallah, M.H. The typology of technology clusters and its evolution — evidence from the hi-tech industries. *Technological Forecasting & Social Change*, *78*, 6 (2011), 945-952.

28. Huma, Z.-E.; Hussain, S.; Thurasamy, R.; and Malik, M.I. Determinants of cyberloafing: A comparative study of a public and private sector organization. *Internet Research*, *27*, 1 (2017), 97-117.

29. Jarrett, H.M.; Bailie, M.W.; and Hagen, E. Prosecuting computer crimes. Office of Legal Education Executive Office for United States Attorneys, 2010.

30. Jensen, M.L.; Dinger, M.; Wright, R.T.; and Thatcher, J.B. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*, 2 (2017), 597-626.

31. Katz, D., and Kahn, R.L. *The social psychology of organizations*. New York, NY: Wiley, 1966.

32. Khansa, L.; Kuem, J.; Siponen, M.; and Kim, S.S. To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems*, *34*, 1 (2017), 141-176.

33. Kruskal, J.B., and Wish, M. *Multidimensional scaling*. Beverly Hills, London: Sage Publications, 1978.

34. Larsen, K.R.T. A taxonomy of antecedents of information systems success: Variable analysis studies. *Journal of Management Information Systems*, *20*, 2 (2003), 169-246.

35. Liang, N.; Biros, D.P.; and Luse, A. An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*, 2 (2016), 361-392.

36. Lim, V.K.G. The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, *23*, 5 (2002), 675-694.
37. Loch, K.D.; Carr, H.H.; and Warkentin, M.E. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*, 2 (1992), 173-186.
38. Lovelace. Cost of data breaches hits $4 million on average: IBM. Retreived from http://www.cnbc.com/2016/06/14/cost-of-data-breaches-hits-4-million-on-average-ibm.html. Accessed on 1 May, 2017.
39. Lowry, P.B.; Willison, R.; and Paternoster, R. A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems,* (forthcoming).
40. Mandell, M., and Steelman, T. Understanding what can be accomplished through interorganizational innovations the importance of typologies, context and management strategies. *Public Management Review*, *5*, 2 (2003), 197-224.
41. Markus, M. Finding a happy medium: Explaining the negative effects of electronic communication on social life at work. *ACM Transactions on Information Systems (TOIS)*, *12*, 2 (1994), 119-149.
42. Mawritz, M.B.; Greenbaum, R.L.; Butts, M.M.; and Graham, K.A. I just can't control myself: A self-regulation perspective on the abuse of deviant employees. *Academy of Management Journal*, *60*, 4 (2017), 1482-1503.
43. Mayr, E. *Principles of systematic zoology*. New York: McGraw-Hill, 1969.
44. McKelvey, B. Organizational systematics: Taxonomic lessons from biology. *Management Science*, *24*, 13 (1978), 1428-1440.
45. McKelvey, B. *Organizational systematics: Taxonomy, evolution, classification*. Berkeley, CA: University of California Press, 1982.
46. McKinney, E.H., and Yoos, C.J. Information about information: A taxonomy of views. *MIS Quarterly*, *34*, 2 (2010), 329-344.
47. McKinney, J.C. Typification, typologies, and sociological theory. *Social Forces*, *48*, 1 (1969), 1-12.
48. Miller, J.G., and Roth, A.V. A taxonomy of manufacturing strategies. *Management Science*, *40*, 3 (1994), 285-304.
49. Moody, G.D.; Siponen, M.; and Pahnila, S. Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*, 1 (2018), 285-311.
50. Moores, T.T., and Chang, J.C.-J. Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, *30*, 1 (2006), 167-180.
51. Morgan, D.L. *Focus groups as qualitative research*. Thousand Oaks, Calif: Sage Publications, 1997.
52. O'Neill, T.A.; Hambley, L.A.; and Bercovich, A. Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, *34* (2014), 291-298.
53. Patrick, E. Employee Internet management: Now an HR issue. Retreived from https://www.shrm.org/hr-today/news/hr-magazine/pages/cms_006514.aspx. Accessed on 20 December, 2016.
54. Peace, A.G.; Galletta, D.F.; and James, Y.L.T. Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, *20*, 1 (2003), 153-177.

55. Pearce, P.L., and Amato, P.R. A taxonomy of helping: A multidimensional scaling analysis. *Social Psychology Quarterly*, *43*, 4 (1980), 363-371.

56. Pillemer, J., and Rothbard, N.P. Friends without benefits: Understanding the dark sides of workplace friendship. *Academy of Management Review,* (forthcoming).

57. Piotrowski, C. From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations. *Organization Development Journal*, *30*, 4 (2012), 44-53.

58. PonemonInstitute. 2016 cost of data breach study: Canada Michigan, USA: Ponemon Institute LLC, 2016.

59. Posey, C.; Roberts, T.; Lowry, P.; Bennett, B.; and Courtney, J. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*, 4 (2013), 1189-1210.

60. Prat, N.; Comyn-Wattiau, I.; and Akoka, J. A taxonomy of evaluation methods for information systems artifacts. *Journal of Management Information Systems*, *32*, 3 (2015), 229-267.

61. Rest, J.R. The major components of morality. In, Kurtines, W.M., and Gewitz, J.L., (eds.), *Morality, moral behavior, and moral development*, New York, NY: Wiley, 1984, pp. 24-38.

62. Robert Jr, L.P., and Sykes, T.A. Extending the concept of control beliefs: Integrating the role of advice networks. *Information Systems Research*, *28*, 1 (2016), 84-96.

63. Robinson, S.L., and Bennett, R.J. A typology of deviant workplace behaviors: A multidimensional scaling study. *The Academy of Management Journal*, *38*, 2 (1995), 555-572.

64. Robinson, S.L., and Bennett, R.J. Workplace deviance: It's definition, it's manifestations, and it's causes. In, Lewicki, R.J., Sheppard, B.H., and Bies, R.J., (eds.), *Research on negotiation in organizations*, Greenwich, CT: JAI Press, 1997, pp. 3-27.

65. Sarker, S.; Ahuja, M.; and Sarker, S. Work–life conflict of globally distributed software development personnel: An empirical investigation using border theory. *Information Systems Research*, *29*, 1 (2018), 103-126.

66. Shamsudin, F.M.; Subramaniam, C.; and Alshuaibi, A.S. The effect of HR practices, leadership style on cyberdeviance: The mediating role of organizational commitment. *Journal of Marketing & Management*, *3*, 1 (2012), 22-48.

67. Sojer, M.; Alexy, O.; Kleinknecht, S.; and Henkel, J. Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code. *Journal of Management Information Systems*, *31*, 3 (2014), 287-325.

68. Son, J.-Y., and Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, *32*, 3 (2008), 503-529.

69. Sproull, L., and Kiesler, S. Reducing social context cues: Electronic mail in organizational communication. *Management Science*, *32*, 11 (1986), 1492-1512.

70. Straub, D.W.; Carlson, P.; and Jones, E. Deterring highly motivated computer abusers: A field experiment in computer security. In, Gable, G.G., and Caelli, W.J., (eds.), *IT security: The need for international cooperation*, Amsterdam, Holland: North Holland Publishing, 1992, pp. 309-324.

71. Straub, D.W., and Nance, W.D. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*, 1 (1990), 45-60.

72. Straub, D.W., and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*, 4 (1998), 441-469.

73. Sussman, S.W., and Sproull, L. Straight talk: Delivering bad news through electronic communication. *Information Systems Research*, *10*, 2 (1999), 150-166.

74. Sykes, T.A., and Venkatesh, V. Explaining post-implementation employee system use and job performance: Impacts of the content and source of social network ties. *MIS Quarterly*, *4*, 3 (2017), 917-936.

75. Tams, S.; Thatcher, J.B.; and Grover, V. Concentration, competence, confidence, and capture: An experimental study of age, interruption-based technostress, and task performance. *Journal of the Association for Information Systems,* (forthcoming).

76. Thompson, P. Some missing data patterns for multidimensional scaling. *Applied Psychological Measurement*, *77*, 1 (1983), 45-55.

77. Thong, J.Y.; Venkatesh, V.; Xu, X.; Hong, S.J.; and Tam, K.Y. Consumer acceptance of personal information and communication technology services. *IEEE Transactions on Engineering Management*, *58*, 4 (2011), 613-625.

78. U.S. Department of Justice. 2015 Internet crime report. 2015.

79. U.S. Department of Justice. Prosecuting computer crimes. Computer crime and intellectual property division. Washington D.C. : Office of the Legal Education, 2007.

80. Ulrich, D., and McKelvey, B. General organizational classification: An empirical test using the united states and japanese electronics industries. *Organization Science*, *1*, 1 (1990), 99-118.

81. van Dyne, L.; Cummings, L.L.; and McLean-Parks, J.M. Extra-role behaviors: In pursuit of construct and definitional clarity. In, Cummings, L.L., and Staw, B.M., (eds.), *Research in organizational behavior*, Greenwich, CT: JAI Press, 1995, pp. 215-285.

82. Vance, A.; Lowry, P.B.; and Eggett, D. Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*, 2 (2015), 345-366.

83. Venkatesh, V.; Bala, H.; and Sambamurthy, V. Implementation of an information and communication technology in a developing country: A multimethod longitudinal study in a bank in India. *Information Systems Research*, *27*, 3 (2016), 558-579.

84. Venkatesh, V.; Morris, M.G.; Davis, G.B.; and Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 3 (2003), 425-478.

85. Venkatesh, V.; Thong, J.Y.; and Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*, 1 (2012), 157-178.

86. Venkatesh, V.; Thong, J.Y.; and Xu, X. Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*, 5 (2016), 328-376.

87. Vitak, J.; Crouse, J.; and LaRose, R. Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*, 5 (2011), 1751-1759.

88. Weatherbee, T., and Kelloway, E.K. A case of cyberdeviance: Cyberaggression in the workplace. In, Kelloway, E.K., Barling, J., and Hurrell, J.H., (eds.), *Handbook of workplace violence*, Newbury Park, CA: Sage Publications, 2006, pp. 445-487.

89. Weatherbee, T.G. Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*, 1 (2010), 35-44.

90. Whitty, M.T., and Carr, A.N. New rules in the workplace: Applying object-relations theory to explain problem internet and email behaviour in the workplace. *Computers in Human Behavior*, *22*, 2 (2006), 235-250.

91. Willison, R., and Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*, 1 (2013), 1-20.

92. Xu, X.; Thong, J. Y.; and Venkatesh, V. Effects of ICT service innovation and complementary strategies on brand equity and customer loyalty in a consumer technology market. *Information Systems Research*, *25*, 4 (2014), 710-729.

93. Xu, X.; Venkatesh, V.; Tam, K.Y.; and Hong, S.J. Model of migration and use of platforms: Role of hierarchy, current generation, and complementarities in consumer settings. *Management Science*, *56*, 8 (2010), 1304-1323.

94. Yam, K.C.; Klotz, A.C.; He, W.; and Reynolds, S.J. From good soldiers to psychologically entitled: Examining when and why citizenship behavior leads to deviance. *Academy of Management Journal*, *60*, 1 (2017), 373-396.

95. Yang, J., and Diefendorff, J.M. The relations of daily counterproductive workplace behavior with emotions, situational antecedents, and personality moderators: A diary study in hong kong. *Personnel Psychology*, *62*, 2 (2009), 259-295.

96. Zhang, X., and Venkatesh, V. A nomological network of knowledge management system use: Antecedents and consequences. *MIS Quarterly*, *41*, 4 (2017), 1275-1306.

97. Zhao, X.; Xue, L.; and Whinston, A.B. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*, 1 (2013), 123-152.

Appendix A: Prior Studies of Negative IT Use in the Workplace from ISR, JAIS, JMIS and MISQ (1997 to 2018)

Authors	Journal	Topic	Theory	Research Design	Technology
Addas and Pinsonneault [1]	MISQ	E-mail interruptions	Action regulation theory	Survey; diary	E-mail
Anandarajan [2]	JMIS	Nonwork web surfing	Artificial intelligence-based model	Survey; design science	Web
Angst et al. [3]	MISQ	Data security breach	Institutional theory	Archival data	IT security technologies in hospitals
Ayyagari et al. [4]	MISQ	Technostress	The person–environment fit model	Survey	NONE
Banerjee et al. [5]	MISQ	IT ethics behavior	Theory of planned behavior	Survey	NONE
Barlow et al. [6]	JAIS	Information security compliance	Anti-neutralization, informational, and normative communication approaches	Survey	NONE
Bulgurcu et al. [7]	MISQ	Information security policy compliance	Theory of planned behavior	Survey	NONE
Chidambaram and Tung [8]	ISR	Social loafing	Social impact theory	Experiment	Technology-supported groups
Culnan and Williams [9]	MISQ	Data breach	NONE	Case study	NONE
D'Arcy et al. [10]	ISR	IS misuse	Extended deterrence theory model	Survey	Computers at work
George et al. [11]	JAIS	Deception	Interpersonal deception theory	Experiment	Group support systems
Guo et al. [12]	JMIS	Nonmalicious security violation	The composite behavior model	A scenario-based survey	NONE
Gwebu et al. [13]	JMIS	Data breach	Cognitive dissonance theory	Event study	NONE
Hu et al. [14]	JMIS	Information security violations	Self-control theory	Scenario-based laboratory experiments	NONE
Jensen et al. [15]	JMIS	Phishing	Mindfulness theory	Experiment	E-mail
Johnston and Warkentin [16]	MISQ	Information security behavior	Protection motivation theory; fear appeal theories	Experiment	Anti-spyware software
Khansa et al. [17]	JMIS	Cyberloafing	Social learning theory	Longitudinal survey	Internet
Liang et al. [18]	ISR	IT compliance	Regulatory focus theory	Survey	ERP
Lowry et al. [19]	JAIS	Internal computer abuse	Deterrence theory; rational choice theory	Literature review	NONE
Menard et al. [20]	JMIS	Information security behavior	Protection motivation theory; self-determination theory	Experiment	NONE
Moody et al. [21]	MISQ	Information security policy compliance	The unified model of information security policy compliance	Survey	Information security policy
Moores and Chang [22]	MISQ	Software piracy	The four-component model of morality	A scenario-based survey	Software
Peace et al. [23]	JMIS	Software piracy	Theory of planned behavior; expected utility theory; deterrence theory	Survey	Software
Posey et al. [24]	JMIS	Information security threats	Protection motivation theory	Survey	NONE
Puhakainen and	MISQ	Employee	Elaboration likelihood	Action research	Information systems

Authors	Journal	Topic	Theory	Research Design	Technology
Siponen [25]		noncompliance with information systems security policies	model; universal constructive instructional theory		security policy
Ragu-Nathan et al. [26]	ISR	Technostress	Stress	Survey	Computers at work
Sarker et al. [27]	ISR	Work-life conflict	Border theory	Case study; survey	Globally distributed software development
Siponen and Vance [28]	MISQ	Employees' failure to comply with IS security policies	Deterrence theory	A hypothetical scenario method	NONE
Smith et al. [29]	MISQ	IS security compliance	Circuits of power framework	Survey; interview; observation; focus group	NONE
Sojer et al. [30]	JMIS	Unethical programming behavior	Theory of planned behavior	Survey	Programming software
Spears and Barki [31]	MISQ	IS security risk management	Buy-in theory; system quality theory; emergent interactions theory	Interview; survey	NONE
Stein et al. [32]	MISQ	Nonconforming use patterns	A coping model of user adaptation	An in-depth field study	A software package
Tams et al. [33]	JAIS	Interruption-based technostress	Theories of stress and cognitive aging	Experiment	NONE
Vance et al. [34]	JAIS	Information security behavior	Theory of planned behavior; context-updating theory	Experiment	NONE
Vance et al. [35]	MISQ	System access-policy violations	Accountability theory	A scenario-based factorial survey method	A records system containing sensitive information
Wang et al. [36]	MISQ	Insider threats	Routine activity theory	An analysis of log data	An enterprise single sign-on (ESSO) system
Warkentin et al. [37]	JAIS	Secure IT behaviors	Fear appeal theory	Experiment	NONE
Willison and Warkentin [38]	MISQ	Employee computer abuse	Security action cycle framework	NONE	NONE
Wright et al. [39]	ISR	Phishing	Persuasion and motivation theory	A field experiment	E-mail

REFERENCES

1. Addas, S., and Pinsonneault, A. E-mail interruptions and individual performance: Is there a silver lining? *MIS Quarterly*, *42*, 2 (2018), 381-405.

2. Anandarajan, M. Profiling web usage in the workplace: A behavior-based artificial intelligence approach. *Journal of Management Information Systems*, *19*, 1 (2002), 243-266.

3. Angst, C.M.; Block, E.S.; D'Arcy, J.; and Kelley, K. Data security breach, institutional theory, firm characteristics, IT security, health IT, panel data, growth mixture model, longitudinal. *MIS Quarterly*, *41*, 3 (2017), 893-916.

4. Ayyagari, R.; Grover, V.; and Purvis, R. Technostress: Technological antecedents and implications. *MIS Quarterly*, *35*, 4 (2011), 831-858.

5. Banerjee, D.; Cronan, T.P.; and Jones, T.W. Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, *22*, 1 (1998), 31-60.

6. Barlow, J.; Warkentin, M.; Ormond, D.; and Dennis, A.R. Don't even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems,* (forthcoming).

7. Bulgurcu, B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 3 (2010), 523-548.

8. Chidambaram, L., and Tung, L.L. Is out of sight, out of mind? An empirical study of social loafing in technology-supported groups. *Information Systems Research*, *16*, 2 (2005), 149-168.

9. Culnan, M.J., and Williams, C.C. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, *33*, 4 (2009), 673-687.

10. D'Arcy, J.; Hovav, A.; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 1 (2009), 79-98.

11. George, J.F.; Marett, K.; and Giordano, G. Deception: Toward an individualistic view of group support systems. *Journal of the Association for Information Systems*, 9, 10/11 (2008), 653-676.

12. Guo, K.H.; Yuan, Y.; Archer, N.P.; and Connelly, C.E. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*, 2 (2011), 203-236.

13. Gwebu, K.L.; Wang, J.; and Wang, L. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*, 2 (2018), 683-714.

14. Hu, Q.; West, R.; and Smarandescu, L. The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*, 4 (2015), 6-48.

15. Jensen, M.L.; Dinger, M.; Wright, R.T.; and Thatcher, J.B. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*, 2 (2017), 597-626.

16. Johnston, A.C., and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*, 3 (2010), 549-566.

17. Khansa, L.; Kuem, J.; Siponen, M.; and Kim, S.S. To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems*, *34*, 1 (2017), 141-176.

18. Liang, H.; Xue, Y.; and Wu, L. Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research*, *24*, 2 (2013), 279-294.

19. Lowry, P.B.; Willison, R.; and Paternoster, R. A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems,* (forthcoming).

20. Menard, P.; Bott, G.J.; and Crossler, R.E. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*, 4 (2017), 1203-1230.

21. Moody, G.D.; Siponen, M.; and Pahnila, S. Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*, 1 (2018), 285-311.

22. Moores, T.T., and Chang, J.C.-J. Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, 30, 1 (2006), 167-180.

23. Peace, A.G.; Galletta, D.F.; and James, Y.L.T. Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, *20*, 1 (2003), 153-177.

24. Posey, C.; Roberts, T.L.; and Lowry, P.B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*, 4 (2015), 179-214.

25. Puhakainen, P., and Siponen, M. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*, 4 (2010), 757-778.

26. Ragu-Nathan, T.; Tarafdar, M.; Ragu-Nathan, B.S.; and Tu, Q. The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research*, *19*, 4 (2008), 417-433.

27. Sarker, S.; Ahuja, M.; and Sarker, S. Work–life conflict of globally distributed software development personnel: An empirical investigation using border theory. *Information Systems Research*, *29*, 1 (2018), 103-126.

28. Siponen, M., and Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*, 3 (2010), 487-502.

29. Smith, S.; Winchester, D.; Bunker, D.; and Jamieson, R. Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, *34*, 3 (2010), 463-486.

30. Sojer, M.; Alexy, O.; Kleinknecht, S.; and Henkel, J. Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code. *Journal of Management Information Systems*, *31*, 3 (2014), 287-325.

31. Spears, J.L., and Barki, H. User participation in information systems security risk management. *MIS Quarterly*, *34*, 3 (2010), 503-522.

32. Stein, M.-K.; Newell, S.; Wagner, E.L.; and Galliers, R.D. Coping with information technology: Mixed emotions, vacillation, and nonconforming use patterns. *MIS Quarterly*, *39*, 2 (2015), 367-392.

33. Tams, S.; Thatcher, J.B.; and Grover, V. Concentration, competence, confidence, and capture: An experimental study of age, interruption-based technostress, and task performance. *Journal of the Association for Information Systems,* (forthcoming).

34. Vance, A.; Anderson, B.B.; Kirwan, C.B.; and Eargle, D. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*, 10 (2014), 679-722.

35. Vance, A.; Lowry, P.B.; and Eggett, D. Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*, 2 (2015), 345-366.

36. Wang, J.; Gupta, M.; and Rao, H.R. Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*, 1 (2015), 91-112.

37. Warkentin, M.; Johnston, A.C.; Walden, E.; and Straub, D.W. Neural correlates of protection motivation for secure IT behaviors: An FMRI examination. *Journal of the Association for Information Systems*, *17*, 3 (2016), 194-215.

38. Willison, R., and Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*, 1 (2013), 1-20.

39. Wright, R.T.; Jensen, M.L.; Thatcher, J.B.; Dinger, M.; and Marett, K. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*, 2 (2014), 385-400.